

April 29, 2019

The Honorable Floyd Prozanski
Chair, Senate Judiciary Committee
900 Court St. NE
Salem, Oregon 97301

**RE: HB 2395 - RELATING TO SECURITY MEASURES REQUIRED FOR DEVICES
THAT CONNECT TO THE INTERNET – OPPOSE UNLESS AMENDED**

Dear Senator Prozanski:

Global Automakers, www.globalautomakers.org, is writing to inform you of **our opposition to HB 2395**, which requires manufactures of connected devices to equip the connected device with certain security features.

Global Automakers represents the U.S. operations of international motor vehicle manufacturers, original equipment suppliers, and other automotive-related trade associations. Our goal in Oregon (and elsewhere) is to foster an open and competitive automotive marketplace and to create public policy that improves motor vehicle safety, encourages technological innovation and protects our planet. Our members manufactured 53% of all new vehicles sold in the state and 61% of all green vehicles.

Our Position

Global Automakers opposes HB 2395 in its current form. While HB 2395 was amended in the House to provide certain exemptions, the bill still lacks notable language that was included in the California legislation, which HB 2395 is based on. Like the California legislation, HB 2395 imposes vague and open-ended requirements that will require manufacturers to grapple with its interpretation when designing product security features.

However, HB 2395 lacks clarifying language which is included in California’s legislation. Accordingly, we request that Section 1(2)(b) be amended as follows: “b) Compliance with requirements of federal law or federal regulations *or adherence to federal guidelines or applicable industry standards* that apply to security measures connected devices.” This amended language would include automobiles because they are already covered by cybersecurity best practice guidance published by the National Highway Traffic Safety Administration.¹

Global Automakers and our members believe that by proactively and collaboratively addressing potential cybersecurity challenges the industry can continue producing safe vehicles that incorporate modern and robust security protections. Our commitment to this proactive approach was demonstrated by the formation of an Automotive Information Sharing and Analysis Center

¹ https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

(Auto-ISAC). The Auto-ISAC is an industry-driven community that shares and analyzes intelligence about emerging cybersecurity risks to the vehicle and seeks to collectively enhance vehicle cybersecurity capabilities.

Our members have also identified industry best practices for vehicle cybersecurity. To support our commitment to enhancing cybersecurity, the members of the Auto Alliance and Global Automakers have developed a Framework for Automotive Cybersecurity Best Practices. The Framework is intended to support the ongoing efforts of the automobile industry on cybersecurity matters. The Framework draws upon established cybersecurity frameworks as well as upon existing cybersecurity measures that have already been implemented by many automakers.

While the California law has serious problems with its overbroad and vague language, the amended language we recommend above provides a crucial level of clarity for manufacturers which is missing in HB 2395. At a minimum, HB 2395 should be amended to include this language.

Global Automakers looks forward to working with members of the Oregon legislature to address these issues.

Please let us know if you have any questions.

Sincerely,



Josh Fisher
Senior Manager, State Government Affairs